REMARKS

Claims 1-43 remain pending in the application.

35 USC 112 Second Paragraph Rejection of Claims 1-27

The Office Action rejected claims 1-35 as allegedly being indefinite under 35 USC 112.

In particular, claims 1-27 were rejected for allegedly lacking antecedent clarity for "said received out-of-order message".

Claims 1-27 are amended herein to clarify antecedent basis.

In particular, claims 1-35 were rejected for allegedly lacking antecedent clarity for "said nonce value".

Claims 1-35 are amended herein to clarify antecedent basis.

In particular, claims 36-43 were rejected for allegedly lack of antecedent basis for "said largest sequence number yet seen".

Claims 36-43 are amended herein to clarify antecedent basis.

It is respectfully submitted that claims 1-35 are now in full conformance with 35 USC 112. It is respectfully requested that the rejection be withdrawn.

Claims 1-43 over Hughes

In the Office Action, claims 1-43 were rejected under 35 U.S.C. §102(b) as allegedly being anticipated by *Combined DES-CBC, HMAC and Replay Prevention Security Transform* to J. Hughes ("Hughes"). The Applicants respectfully traverse the rejection.

Claims 1-27 recite a system and method comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**.

Hughes at pages 3 and 4 discloses a method of preventing attack. A 32 bit incrementing counter starting at a value of 1 is relied on (See Hughes, page 3). A key is relied on to prevent the counter from wrapping, i.e., the key must be changed before (2^{32})-2 packets are transmitted using this key (See Hughes, page 3). A receiver must verify that for a given SPI the packets received have non-repeating (non-duplicate) counter values (See Hughes, page

3). This can be implemented as a simple increasing count test or the receiver may choose to accept out-of-order packets as long as it is guaranteed that packets can be received only once, with some allowance for duplication (See Hughes, page 3). A sliding receive window assists in determining if a received out-of-order packet is received more than once (See Hughes, page 3). Hughes at page 4 simply describes what a payload is, what padding is and what pad length is.

Hughes discloses two types of analysis for a received packet, 1) that the received in-order packets have increasing counter values or 2) for out-of-order packets, that the received packets are received only once by checking for non-repeating counter values within a sliding window, with some allowance for repetition (See Hughes, page 3). For out-of-order packets, Hughes determines that the received out-of-order packets are received only once by checking for non-repeating counter values within a sliding window. Thus, Hughes discloses comparing a counter value of a received out-of-order packet with **all** other values received within a sliding window to check for repetition in a counter value, i.e., fails to disclose or suggest comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**, as recited by claims 1-27.

As the Applicants **previously pointed out**, Hughes discloses analysis of out-of-order packets. However, for out-of-order packets Hughes determines that the received out-of-order packets are **received only once** by checking for **NON-REPEATING** counter values within a sliding window. Thus, Hughes discloses comparing a counter value of a received out-of-order packet with all other values received within a sliding window to check for **repetition** in a counter value, i.e., fails to disclose or suggest comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**, as recited by claims 1-27.

The Examiner alleges in the Response to Arguments section of the Office Action that Hughes' "lastseq" number equates to Applicants' recited largest nonce value **yet seen** (See Office Action, page 9). The Applicants respectfully disagree.

The software routine beginning on page 10 of Hughes is for **in-order** packets. As discussed above, Hughes discloses that in-order packets must have increasing counter values. Hughes' software routine on page 10 simply discloses testing that counter values are increasing by testing a current counter value with a LAST counter value. If the current counter value is larger than the LAST counter value, the software stores the current counter value as lastseq to later test for an increasing counter and return a value of 1 (software routine line 8) indicating that a packet is accepted. Thus, the software routine on page 10 of Hughes assures that received in-order packets have increasing counter values and is **NOT** directed toward out-of-order messages, much less disclose or suggest a system and method comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**, as recited by claims 1-27.

Claims 28-43 recite a system and method of comparing a nonce value to a filter in response to a nonce value of a received **out-of-order** packet not exceeding a largest nonce value **yet seen**.

As discussed above, for out-of-order packets, Hughes determines that the received out-of-order packets are received only once by checking for non-repeating counter values. Thus, Hughes discloses comparing a counter value of a received out-of-order packet with **all** other values received within a sliding window, i.e., fails to disclose or suggest comparing a nonce value to a filter in response to a nonce value of a received **out-of-order** packet not exceeding a largest nonce value **yet seen**, as recited by claims 28-43.

Accordingly, for at least all the above reasons, claims 1-43 are patentable over the prior art of record. It is therefore respectfully requested that the rejection be withdrawn.

Claims 1-43 over Schneier

In the Office Action, claims 1-43 were rejected under 35 U.S.C. §103(a) as allegedly being obvious over U.S. Patent No. 5,970,143 to Schneier et al. ("Schneier"). The Applicants respectfully traverse the rejection.

Claims 1-27 recite a system and method of comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**.

The Examiner alleges Schneier discloses determining a largest nonce value yet seen from a nonce value of a received message and comparing a nonce value of a received message with a largest nonce value yet seen at col. 16, lines 9-16. The Applicants respectfully disagree.

Schneier at col. 16, lines 9-16 discloses a sequence number that is increased by one every time a game computer generates an Authenticatable Outcome Message AOM. A central computer stores the most recent sequence number in memory (See Schneier at col. 16, lines 13-14). The central computer accepts a current outcome message if a sequence number received is **one greater** than the stored sequence number (See Schneier at col. 16, lines 14-16).

As the Examiner correctly **ACKNOWLEGES** in describing what Schneier discloses, Schneier fails to even mention out-of-order messages. Schneier, like Hughes, simply discloses checking for increasing sequence numbers for in-order messages, i.e., **one greater** than the last message. Thus, Schneier fails to even mention out-of-order messages, much less a system and method of comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**, as recited by claims 1-27.

Moreover, the Examiner alleges that Schneier discloses all of the limitations of claims 1-27 (which Schneier fails to do as discussed above), however ACKNOWLEDGES that Schneier discloses the claimed features in DIFFERENT embodiments (See Office Action, page 5). The Examiner alleges the motivation for picking elements from different embodiments to arrive at the claimed features is that it allows old messages which are valid to be allowed if they are within a certain time window and makes the system more robust because it would be able to allow out-of-order messages received within a

certain time window (See Office Action, page 5). The Applicants respectfully disagree.

"The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification." In re Fritch, 23 USPQ2d 1780, 1783-84 (Fed. Cir. 1992). In re Mills, 16 USPQ2d 1430 (Fed. Cir. 1990). Schneier's TWO embodiments are specifically directed toward solving specific problems within the art. **NOTHING** within Schneier **SUGGESTS** the Examiner's modification of picking and choosing elements from the two embodiments to conveniently arrive at the claimed features. "It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious." In re Fritch, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992). If such a modification of Schneier were so obvious from Schneier's disclosed separate embodiments, and since Schneier allegedly discloses **ALL** of the claimed features in separate embodiments, then surely Schneier himself would have arrived at the claimed features. However, Schneier failed to arrive at the claimed features because such a modification of Schneier was **NOT** obvious to one of ordinary skill in the art, much less Schneier. Thus, Schneier fails to **SUGGEST** the alleged taking some elements from one embodiment and taking some elements from a second embodiment to arrive at the claimed features, i.e., fails to suggest a system and method of comparing a nonce value of a received out-of-order message with a largest nonce value **yet seen**, as recited by claims 1-27.

Claims 28-43 recite a system and method of comparing a nonce value to a filter in response to a nonce value of a received **out-of-order** packet not exceeding a largest nonce value **yet seen**.

As discussed above, Schneier simply discloses a system and method to check for increasing sequence numbers for **in-order** messages, i.e., **one greater** than the last message. Schneier fails to even address out-of-order packets, much less disclose or suggest comparing a nonce value to a filter in

response to a nonce value of a received **out-of-order** packet not exceeding a largest nonce value **yet seen**, as recited by claims 28-43.

Accordingly, for at least all the above reasons, claims 1-43 are patentable over the prior art of record. It is therefore respectfully requested that the rejection be withdrawn.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the subject application is in condition for allowance and a Notice to that effect is earnestly solicited.

Respectfully submitted,

William H. Bollman
Reg. No.: 36,457
Tel. (202) 261-1020
Fax. (202) 887-0336

MANELLI DENISON & SELTER PLLC
2000 M Street, NW 7TH Floor
Washington, DC 20036-3307
TEL. (202) 261-1020
FAX. (202) 887-0336

WHB/df